



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/526,169

11/17/2005

Chin Shyan Ooi

7404P001

6494

8791

7590

07/24/2009

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER

SU, SARAH

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

07/24/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/526,169	Applicant(s) OOI ET AL.	
	Examiner Sarah Su	Art Unit 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 May 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-5,7-17,19,21-24 and 27-30 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1, 3-5, 7-17, 19, 21-24, 27-30 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>7/13/09</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11 May 2009 has been entered. In this amendment, claims 1, 7, 16, and 19 have been amended.
2. Claims 1, 3-5, 7-17, 19, 21-24, and 27-30 are presented for examination.

Response to Arguments

3. With regards to the objections to the specification and claims, the applicant has submitted amendments, and the examiner hereby withdraws the objections.
4. Applicant's arguments with respect to claims 1, 3-5, 7-17, 19, 21-24, and 27-30 have been considered but are moot in view of the new ground(s) of rejection.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 13 July 2009 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1, 3-5, 7-9, 13, 15-17, 19, 21-24, and 27-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brandys (WO 02/073877 A2) in view of Horne (US Patent 4,887,296) and further in view of Montenegro et al. (US Patent 7,434,051 B1 and Montenegro hereinafter).

As to claims 1 and 16, Brandys discloses a system and method for authenticating users and data, the system and method having:

a portable data storage device including a non-volatile memory to store data (page 7, lines 8-12);

an interface section to receive data from and transmit data to a host (page 4, lines 3-4);

a master control unit to transfer data to and from the non-volatile memory (page 4, lines 2-3; page 10, lines 25-26);

integrated circuit for generating at least one key (page 4, lines 1-2);

a host computer, the host computer being arranged to transmit a command to the portable data storage device using the interface section to request the data (page 4, lines 17-18).

Brandys fails to specifically disclose:

the portable data storage device being arranged, upon receiving the command from the host requesting the data stored in the non-volatile memory, the data stored prior to receiving the command, to generate the at least one key, to encrypt the generated key using a secret key that is permanently stored in the portable storage device and to transmit the encrypted key and the requested data stored in the non-volatile memory to the host using the interface section, wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key,

wherein the portable data storage device is further arranged to receive from the host a digital signature based on the generated key and the requested data transmitted to the host from the portable storage device, the portable storage device, based on the digital signature, to verify that the requested data has been correctly received by the host.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as taught by Horne.

Horne discloses a system and method for a three key cryptographic system for direct broadcast satellite system, the system and method having:

the portable data storage device being arranged, upon receiving the command from the host requesting the data stored in the non-volatile memory, the data stored prior to receiving the command, to generate the at least one key (i.e. subscriber unit signature key), to encrypt the generated key

Art Unit: 2431

using a secret key (i.e. master factory key) that is permanently stored in the portable storage device (col. 7, lines 57-62) and to transmit the encrypted key and the requested data (i.e. data stream) stored in the non-volatile memory to the host using the interface section, wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key (col. 7, lines 23-29; col. 8, lines 23-31).

Given the teaching of Horne, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Horne by creating a key in order to verify a digital signature. Horne recites motivation by disclosing that protecting a different key for each subscriber unit is burdensome and encrypting unit keys with a master key requires only a single master factory key to be protected (col. 7, lines 12-17). It is obvious that the teachings of Horne would have improved the teachings of Brandys by using a master key to encrypt generated keys in order to require only a single key to be protected instead of multiple generated keys.

Brandys in view of Horne fails to specifically disclose:

wherein the portable data storage device is further arranged to receive from the host a digital signature based on the generated key and the requested data transmitted to the host from the portable storage device, the portable storage device, based on the digital signature, to verify that the requested data has been correctly received by the host.

Art Unit: 2431

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Horne, as taught by Montenegro.

Montenegro discloses a system and method for facilitating secure cocktail effect authentication, the system and method having:

wherein the portable data storage device is further arranged to receive from the host a digital signature based on the generated key and the requested data transmitted to the host from the portable storage device, the portable storage device, based on the digital signature, to verify that the requested data has been correctly received by the host (col. 5, lines 28-37).

Given the teaching of Montenegro, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Horne with the teachings of Montenegro by verifying a received signature based on a key and data. Montenegro recites motivation by disclosing that using a signature generated by received information allows for a requesting device to verify that a responding device is not simply replaying an intercepted message and that the message is legitimate (col. 5, lines 34-37). It is obvious that the teachings Montenegro would have improved the teachings of Brandys in view of Horne by verifying a received signature based on a key and data in order to allow a device to verify that the message is legitimate and has not been intercepted.

Art Unit: 2431

As to claim 19, Brandys discloses:

the portable data storage device generating at least one key (page 4, lines 1-2);

the portable data storage device obtaining the requested data from the non-volatile memory and the portable data storage device transmitting to the host the requested data and the encrypted key (page 3, line 35; page 4, lines 1-4, 17-23);

the host decrypting the encrypted key using the secret key permanently stored in the host (page 6, line 18). The examiner asserts that it would have been well known to one of ordinary skill in the art at the time the invention was made to use either symmetric keys, where the same key is used from encryption and decryption, or asymmetric keys for encryption/decryption because they are functionally equivalent.

the host generating a digital signature based on the decrypted key and the requested data (page 6, lines 19-21).

Brandys fails to specifically disclose:

the portable data storage device receiving and instruction from the host requesting the data stored in a non-volatile memory of the portable data storage device, wherein the data is stored prior to receiving the instruction;

the portable data storage device encrypting the generated key using the secret key permanently stored in the portable data storage device,

wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key;

the host transmitting the digital signature from the host to the portable data storage device;

the portable data storage device using the digital signature to verify that the requested data has been correctly received by the host.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as taught by Horne.

Horne discloses:

the portable data storage device receiving and instruction from the host requesting the data stored in a non-volatile memory of the portable data storage device, wherein the data is stored prior to receiving the instruction (col. 5, lines 16-18);

the portable data storage device encrypting the generated key (i.e. subscriber unit signature key) using the secret key (i.e. master factory key) permanently stored in the portable data storage device, wherein the secret key is permanently stored within the portable storage device prior to the generating at least one key (col. 7, lines 23-29; col. 8, lines 23-31).

Given the teaching of Horne, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Horne by creating a key in order to verify a digital signature. Please refer to the motivation recited above with respect to claims 1

Art Unit: 2431

and 16 as to why it is obvious to apply the teachings of Horne to the teachings of Brandys.

Brandys in view of Horne fails to specifically disclose:

the host transmitting the digital signature from the host to the portable data storage device;

the portable data storage device using the digital signature to verify that the requested data has been correctly received by the host.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Horne, as taught by Montenegro.

Montenegro discloses:

the host transmitting the digital signature from the host to the portable data storage device (col. 5, lines 28-31);

the portable data storage device using the digital signature to verify that the requested data has been correctly received by the host (col. 5, lines 34-37).

Given the teaching of Montenegro, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Horne with the teachings of Montenegro by using a received digital signature for verification. Please refer to the motivation

Art Unit: 2431

recited above with respect to claims 1 and 16 as to why it is obvious to apply the teachings of Montenegro to the teachings of Brandys in view of Horne.

As to claims 3 and 22, Brandys discloses:

wherein the digital signature is produced by hashing the received data to generate a hash result, and encrypting the hash result using the generated key (page 4, lines 19-23).

As to claims 4 and 23, Brandys discloses:

wherein the generated key is the private key of a public key/private key pair (page 4, lines 1-3).

As to claims 5 and 24, Brandys discloses:

wherein the verification of the digital signature is performed in the portable data storage device using the public key (page 5, line 35).

As to claims 7 and 27, Brandys discloses:

wherein the requested data includes both data present in the non-volatile memory, and also biometric data obtained from a biometric sensor of the portable data storage device (page 2, lines 24-26).

As to claims 8 and 28, Brandys fails to specifically disclose:

the requested data is transmitted from the portable data storage device to the host in an encrypted form.

Art Unit: 2431

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys, as taught by Horne.

Horne discloses:

the requested data is transmitted from the portable data storage device to the host in an encrypted form (col. 7, lines 23-25).

Given the teaching of Horne, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys with the teachings of Horne by transmitting encrypted data.

Horne recites motivation by disclosing that encrypting data using an individualized key allows portions of the data to be received only by a particular subscriber unit (col. 7, lines 42-45). It is obvious that the teachings of Horne would have improved the teachings of Brandys by transmitting encrypted data in order to allow only certain units to receive the data.

As to claims 9 and 29, Brandys discloses:

a biometric sensor (page 3, lines 14-15);

a verification engine for granting access to data stored in the portable data storage device based on a biometric verification of the user's identity by comparison of biometric data received using the biometric sensor with pre-stored biometric data (page 2, lines 24-26).

As to claim 13, Brandys discloses:

the interface section is for wireless communication with the host
(page 3, lines 11-12).

As to claim 15, Brandys discloses:

a camera for generating image data, and/or a microphone for capturing audio data (page 7, lines 19-20), **the master control unit being arranged to store the image data and/or the audio data in the memory** (page 7, lines 8-12).

As to claim 17, Brandys discloses:

wherein the generated key is one key of a public key/private key pair (page 4, lines 1-3), **and the host is arranged to generate a digital signature using the private key and the requested data** (page 6, lines 19-21).

As to claim 21, Brandys discloses:

wherein the host generates the digital signature using the private key and the requested data (page 4, lines 19-21).

8. Claims 10 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brandys in view of Horne and Montenegro as applied to claims 1 and 19 above, and further in view of Iwagaki et al. (US 2003/0161468 A1 and Iwagaki hereinafter).

As to claims 10 and 30, Brandys in view of Horne and Montenegro fails to specifically disclose:

a compression algorithm for exploiting any redundancy in data received by the portable data storage device to compress it before storing

it in the non-volatile memory, and a decompression engine to regenerate the data before it is transmitted from the portable data storage device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Horne and Montenegro, as taught by Iwagaki.

Iwagaki discloses a system and method for securing a storage device, the system and method having:

a compression algorithm for exploiting any redundancy in data received by the portable data storage device to compress it before storing it in the non-volatile memory, and a decompression engine to regenerate the data before it is transmitted from the portable data storage device

(0009, lines 13-17).

Given the teaching of Iwagaki, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Horne and Montenegro with the teachings of Iwagaki by providing for compression and decompression of stored data. Iwagaki recites motivation by disclosing that data can be very large and storing uncompressed data in a storage device does not effectively utilize the storage capacity of the device (0009, lines 9-12). It is obvious that the teachings of Iwagaki would have improved the teachings of Brandys in view of Horne and Montenegro by allowing for the compression and decompression of stored data in order to use the storage capacity of the device more effectively.

9. Claims 11, 12, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brandys in view of Horne and Montenegro as applied to claim 1 above, and further in view of Fang (US Patent 6,536,941 B1).

As to claim 11, Brandys in view of Horne and Montenegro fails to specifically disclose:

the interface section includes a USB connector and a USB interface device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Horne and Montenegro, as taught by Fang.

Fang discloses a wrist-worn personal flash disk apparatus, the apparatus having:

the interface section includes a USB connector and a USB interface device (col. 1, lines 37-41).

Given the teaching of Fang, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Horne and Montenegro with the teachings of Fang by allowing connectively through USB. Fang recites motivation by disclosing using a USB interface allows for easy establishment of a link to a host computer so that data can be read or written (col. 1, lines 38-39). It is obvious that the teachings of Fang would have improved the teachings of Brandys in view of Horne and Montenegro by providing for an interface using USB in order to allow for easy connectivity to a host.

Art Unit: 2431

As to claim 12, Brandys in view of Horne and Montenegro fails to specifically disclose:

the connector is a USB plug integral with the portable data storage device.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Horne and Montenegro, as taught by Fang.

Fang discloses:

the connector is a USB plug integral with the portable data storage device (col. 1, lines 37-41).

Given the teaching of Fang, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Horne and Montenegro with the teachings of Fang by providing for a USB connection for the device. Please refer to the motivation recited above with respect to claim 11 as to why it is obvious to apply the teachings of Fang to the teachings of Brandys in view of Horne and Montenegro.

As to claim 14, Brandys in view of Horne and Montenegro fails to specifically disclose:

a housing, the housing including a narrowed end for use as a pointer.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Brandys in view of Horne and Montenegro, as taught by Fang.

Art Unit: 2431

Fang discloses:

a housing, the housing including a narrowed end for use as a pointer

(33, Figure 1).

Given the teaching of Fang, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Brandys in view of Horne and Montenegro with the teachings of Fang by providing for a housing with a narrowed end. Fang recites motivation by disclosing that the storage device can have multiple functions depending on the physical shape of the device (Abstract, lines 1-14). It is obvious that the teachings of Fang would have improved the teachings of Brandys in view of Horne and Montenegro by providing for a specific shaped housing, such as a narrowed end, in order to allow for multiple functions of the device.

It is also noted that “for use as a pointer” recites intended use and has been given little patentable weight.

Prior Art Made of Record

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Kelly (US Patent 5,636,280) discloses a system and method for dual key reflexive encryption.
- b. Shambroom (US 2001/0020274 A1) discloses a system and method for providing secure remote operations over an insecure computer network.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431